

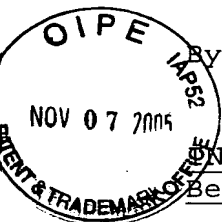
Docket No.: GTP/US 3183

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date indicated below.

MAIL STOP: APPEAL BRIEF-PATENTS

By: 

Date: November 4, 2005



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

Applic. No. : 09/917,541 Confirmation No.: 9996
Inventor : Katrin Reisinger
Filed : July 27, 2001
Title : Mailing Machine and Initialization Method
TC/A.U. : 3621
Examiner : Daniel L. Greene
Customer No. : 24131

Hon. Commissioner for Patents
Alexandria, VA 22313-1450

RESPONSE TO NOTIFICATION OF NON-COMPLIANT APPEAL BRIEF

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S i r :

Responsive to the Notification of Non-Compliant Appeal Brief,
dated October 4, 2005, kindly consider the following:

Remarks/Arguments begin on page 2 of this paper.

Remarks:

Pursuant to an Order of the Board ("Order"), Appellant's Previous Appeal Brief was held to be defective. In response to the Order and to a Notification of Non-Compliant Appeal Brief mailed on October 4, 2005 (the "Notification"), Appellant is filing the present response, accompanied by a Supplemental Appeal Brief.

Pursuant to the Order and Notification, Appellant has been asked to file a Supplemental Appeal Brief in compliance with 37 C.F.R. § 41.37. The Order additionally requires the Examiner to file a Supplemental Answer corresponding to Appellant's Supplemental Appeal Brief.

As such, Appellant is filing the present Supplemental Appeal Brief, which is believed to be in compliance with 37 C.F.R. § 41.37. Appellant's Supplemental Appeal Brief now includes the required Evidence and Related Proceedings Appendices, as well as the other headings in accordance with 37 C.F.R. § 41.37.

Further, in the interest of economy, Appellant has addressed and responded in the Supplemental Appeal Brief, to the Examiner's arguments made in the Examiner's Answer, which Answer was additionally held by the Board to be defective.

It is believed that the Substitute Appeal Brief is proper and addresses all of the issues raised in the **Order** and the **Notification**.

If further information is needed, or the Substitute Appeal Brief is deemed to be insufficient in any way, Appellants request that the Examiner please feel free to contact the Appellants' Attorney by telephone to expedite resolution of these issues.

If an extension of time for this paper is required, petition for extension is herewith made.

Please charge any fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner and Greenberg, P.A., No. 12-1099.

Respectfully submitted,



For Appellants

November 4, 2005

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

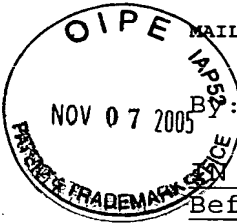
Docket No.: GTP/US 3183

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date indicated below.

MAIL STOP: APPEAL BRIEF-PATENTS

BY: 

Date: November 4, 2005

 THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

Applic. No. : 09/917,541 Confirmation No.: 9996
Inventor : Katrin Reisinger
Filed : July 27, 2001
Title : Mailing Machine and Initialization Method
TC/A.U. : 3621
Examiner : Daniel L. Greene
Customer No. : 24131

Hon. Commissioner for Patents
Alexandria, VA 22313-1450

BRIEF ON APPEAL

S i r :

In response to the *Notification of Non-Compliant Appeal Brief* dated October 4, 2005, Appellants herewith submit a new *Brief on Appeal* in triplicate in compliance with the above-cited notification and with 37 C.F.R. § 41.37.

Payment in the amount of \$500.00 to cover the fee for filing the *Brief on Appeal* was submitted on March 24, 2005.

Real Party in Interest:

This application is assigned to Francotyp-Postalia AG & Co. KG of Birkenwerder, Germany. The assignment will be submitted for recordation upon the termination of this appeal.

Related Appeals and Interferences:

No related appeals or interference proceedings are currently pending which would directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

Status of Claims:

Claims 1-27 are rejected and are under appeal. No claims were cancelled.

Status of Amendments:

No claims were amended after the final Office Action. A *Notice of Appeal* was filed on January 27, 2005. No *Advisory Action* has yet been received.

Summary of the Claimed Subject Matter:

As stated in the first paragraph on page 1 of the specification of the instant application, the invention relates to a mailing machine of the type having a controller, a security module, and a non-removable program memory. The invention further pertains to a method of initializing a

mailing machine of this type. The term mailing machine, as used herein, is to be understood as including, for example, franking machines and postage-calculating scales, i.e. mail scales, with an integrated postage calculator and similar mailing devices for which approval from the postal authorities is required.

Appellant explained on page 15 of the specification, line 2, that, referring now to the figures of the drawing in detail and first, particularly, to Fig. 1 thereof, there is seen a basic diagram with a data source and with a dongle, at the interfaces in each case of the base of a franking machine. The franking machine comprises a meter 1 and a base 2 and is equipped for franking an item of mail 3. A perspective view of the franking machine of the JetMail[®] type is represented from behind in Fig. 3. For its initialization, a data source 4 is connected to a first serial interface 92a of the franking machine. The data source 4 is, for example, a service PC or, preferably, a laptop. A dongle 5 is connected to a second serial interface 98b of the franking machine. The meter 1 of the franking machine has at least one program memory 10 with an initialization program and a security module 11, for checking the authorization before and during the initialization.

It is set forth on page 16 of the specification, line 1, that, in Fig. 3, a perspective view of a franking machine of the JetMail® type from behind is represented. The base 2 of the franking machine has a first serial interface 92a, at which the data source 4 can be connected. Fig. 3 also shows a view of a data source of the laptop type from the front, which can be connected via a cable 41 to the first serial interface 92a of the franking machine. Fitted onto the second serial interface 98b is a dongle 5. Both serial interfaces 92, 98b and further system interfaces 98a and 99a are located on the rear side of the franking machine and are in operative connection with the meter 1. The actuating elements 88 of a keyboard and the display elements 89 in the screen of a display unit of the meter 1 form a user interface, which is configured for the input of INIT values. However, a preferred means of input for the INIT values is the data source 4. The base 2 is equipped with a switch 71 and with a key-operated switch 73, which are arranged behind a guide plate 20 and are accessible from the upper edge 22 of the housing. Once the franking machine has been switched on by means of the switches 71 and 73, a fed-in letter 3, which is standing on edge and bears against the guide plate with its surface onto which printing is to be carried out, then has a franking stamp 31 printed onto it in a way corresponding to the input data. The letter-feeding opening is laterally bounded by a transparent

plate 21 and the guide plate 20. Further stations or items of equipment can be connected to the interfaces 98a and 99a, in order to come into communication link with the franking machine. After the input of initialization data, including a zero credit value, a test takes place. During the franking with the postage value zero, only the value in the number-of-items register is incremented in the accounting operation. The postage value zero is in this case printed onto an item to be dispatched (letter 3).

Appellant outlined on page 17 of the specification, line 9, that, in Fig. 4, a basic diagram with a data source 4 at the interface 92a and with a dongle 5 at the interface 98b of the base 2 of a franking machine is represented. In the configurational variants according to Figs. 1, 3 and 4, it is provided that the data source 4 contains data for initializing the franking machine 1, 2 and is designed such that it can be fitted onto the first interface 92a of the base 2 of the franking machine. The authorization device 5, also referred to as means of authorization or authorization means 5 is designed such that it can be fitted onto a second interface 98b of the base 2 of the franking machine. A dongle 5 preferably serves as the authorization means. Optionally contained in the base 2 are a modem 8 and a further interface 98c for the connection of the integrated modem 8 to a

telephone network. The modem 8 can be used for example to charge an amount of credit from a remote data center into the postal security module 11 of the franking machine. With the postal security module 11, it can also be checked whether the initialization program stored in the program memory 10 is called up in the authorized way and is running properly. In the variant according to Fig. 4, the meter 1 is connected via a further internal serial interface 97a to a chip card reader 70 integrated into the base 2. After completion of the initializing process, a chip card or a smart card (not shown) can be inserted into the slot 72, in order to load further data. Such further data concern, for example, the image data for a predetermined location and date stamp. A method and arrangement for printing-stamp input into a franking machine has already been disclosed in the German patent application with the number 199 13 066.3, which is not a prior publication. Carrier-specific print-image data can be loaded, or selected for a country-specific variant of the franking machine, by means of a chip card.

As described on page 20 of the specification, line 10, Fig. 8 shows a basic diagram with a dongle 5 on a data source 4, which is connected at an interface 92a of the franking machine, and with a chip card reader 70 integrated into the meter 1, although the dongle 5 is the means of authorization.

The means of authorization (dongle) 5 is connected to the data source 4 via a parallel interface. The data source 4 is, for example, a personal computer or, preferably, a laptop. The data source 4 is coupled to the meter 1 via a serial interface 92a of the franking machine. Consequently, as in the configurational variant according to Fig. 2 as well, the means of authorization (dongle) 5 is connected to the franking machine in an indirect way. It is provided that the meter 1 has a program memory 10 for the initialization program and a postal security module 11 as a means for checking the authorization of an input of initialization data, or at least for the authorization of a data input of predetermined INIT values.

Appellant further stated on page 21 of the specification, line 10, that, in Fig. 9, the basic diagram for a configurational variant with a data source 4 connected to the interface 92a of the base 2 of a franking machine and with a chip card reader 70 integrated into the meter is represented, the chip card 49 forming the means of authorization. It is otherwise designed in a way corresponding to the design already explained with reference to Fig. 8.

It is stated in the last paragraph on page 21 of the specification, line 18, that, in Figs. 5, 6, 7 or 9, chip

cards 49 are provided for insertion into the base 2 or into the meter 1 of the franking machine. The chip cards 49 contain, for example:

- a card producer code MANCODE (15 bytes),
- a franking-machine producer code FPCODE (one byte),
- a code for the physical card type PHYSTYP (one byte),
- a personalization code MINIPERS (6 bytes), which includes the code of the producer of the franking machine, the producer of the chip card and the producer of the chip of the chip card in combination,
- a start date for the validity of the card VALSTARTDATE (4 bytes),
- an end date for the validity of the card VALENDDATE (4 bytes),
- an access code LOGICTYPE (1 byte), which shows that an authorization card exists, preferably for the vendor, and
- a unique authorization number (4 bytes) and also
- if appropriate, a country code COUNTRYCODE (4 bytes).

Appellant explained on page 22 of the specification, line 12, that it is provided that checking of the authorization is performed before and during the initialization on the basis of a unique authorization number, which is input via the chip

card 49. Alternatively, the unique authorization number may be input via the dongle 5. The authorization is given if the input unique authorization number has a predetermined relationship with a number stored in the postal security module 11.

Appellant described in the last paragraph on page 22 of the specification, line 20, that, in another configurational variant represented in Fig. 10, the mailing machine is a set of scales 6 and the means of authorization is a chip card 49. A chip card reader 7 is integrated into the scales 6. A franking machine or an external modem (not shown) may be connected, in each case via interface 90 or 91, respectively. The set of scales contains, for example, a postage module 12, which additionally operates as a security module for checking the authorization of initialization data.

As set forth on page 24 of the specification, line 8, the process for initializing a mailing machine has the following steps:

- Switching into an initialization mode;
- Authorization of the initialization by means of a means of authorization, for example a chip card 49 or a dongle 5, and checking of the authorization by means of the

security module 11, in order to prevent initialization without authorization;

- Input of initialization data, which are at least partly supplied by a data source (data center 4). The initialization data may be input from a personal computer (PC) connected to a serial interface. The PC may in turn be connected to a data center 4 by means of a modem or a serial or parallel connection. The mailing machine may, however, also be connected to the data center 4 via a modem, in order that the initialization data can be input into the mailing machine. The initialization data may be codes which are necessary for the encoded transmission of data. Furthermore, equipment and producer IDs stored at the data center 4 may be transmitted, and customer-specific data (for example zip code/postal code), register values (minimum and maximum values for certain registers) may likewise be transmitted. After the transmission of initialization data, the mailing machine is enabled for use by a user. Charging with money is possible and so too is franking.
- Ending of the initialization and cancelling of the authorization by removal of the means of authorization.

Appellant explained on page 25 of the specification, line 11, that, as in Figs. 5, 6, 7 or 9, 10, 11, chip cards 49 are provided as the authorization means 5 and the mailing machine 6, or else the base 2 or the meter 1 of a franking machine, are equipped for the insertion of the chip card 49 with a chip card reader, with a modem interface 98c and with a modem. If the chip cards alone are provided for initialization, a chip card 49 is known as the initialization card (INIT card). All, or at least some, of the INIT data or values are then supplied to the franking machine from the remote data center via the modem interface 98c. The chip card 49 serves for authorizing at least that part of the INIT data or values which is loaded into the franking machine from the remote data center via a modem interface 98c. In Figs. 5 and 7, the modem interface 98c is represented on the rear wall of the JetMail franking machine. In this case it is provided that the associated initialization program is stored at least partly in a program memory (EPROM), which is a component part of the security module 11. Another part of the initialization program, in particular for initialization data which are stored in a non-volatile manner externally of the security module 11, is a component part of a separate program memory (EPROM), which however is in connection with the security module 11. The security module prevents the loading or storing of data which are not authorized by the means of authorization 5 or 49. It

is provided that interrogation of the means of authorization 5 or 49 is performed before and during the initialization of the mailing machine 1, 2 with predetermined INIT data.

As further outlined on page 27 of the specification, line 12, the following information comprises the INIT data which have to be entered into the franking machine during initializing at the point of entry of the respective destination country:

- date of the battery of the security module,
- telephone number of the data center,
- postage call-up number PAN,
- predetermined INIT values and
- extra data and also
- if appropriate, codes at least for remote value input.

Appellant stated on page 29 of the specification, line 7, that, during initializing, at least one common secret code DES-Key is loaded into a secure accounting device SAD, at least for the remote input of a credit when a secret key process is used. Furthermore, a common secret code MAC-Key of a mail carrier, required for generating a security imprint and its checking, may be loaded. The loading and constant

presence of an initialization program in the program memory of the franking machine requires special security measures in the SAD (secure accounting device). For instance, the postal-relevant SAD serial number is pre-initialized already during production and can no longer be changed later unless a new SAD is installed. A serial number of the franking machine is not the same as the SAD serial number and in postal terms is of no further relevance. The franking machine is packed into a box on which a label with the SAD serial number is adhesively attached. The box is dispatched to a destination country remote from the location of production. At the goods receiving location of the destination country (single point of entry), initializing takes place after unpacking. If parameters of the franking machine have to be changed in the initialization mode, a record is kept of who makes these changes. Each dealer card has a unique authorization number for enabling the initialization mode.

As outlined on page 30 of the specification, line 5, during initializing, the following steps are carried out:

- switching a franking machine into an initialization mode, for example as the result of activating a means of activating the user interface, and establishing a

connection to a data source (4) via a modem or by means of a laptop or PC interface;

- authorization of the initialization by means of a means of authorization (5), for example by means of an FP card inserted into the chip card reader;
- input at least of the date BAT_DATE_SAD, for example = 07 00, of the battery of the security module (11) SAD, a telephone number of the telepostage data center TDC of the destination country and a postage call-up number PAN, for example = 101 04711;
- sending of the serial number SAD-SN of the security module (11) to the telepostage data center TDC of the country, a comparison of the serial number SAD-SN sent with a stored serial number taking place there, and a notification being generated;
- reception of a notification sent by the telepostage data center TDC by the franking machine and loading at least of codes DES-Keys for credit recharging into the security module (11) SAD, the latter including: Key(0), Key(1), Kvar;

- ending of the initialization and cancellation of the authorization by removal of the means of authorization (5), for example the FP card.

Appellant stated on page 33 of the specification, line 1, that the automatic installation at the customer's by modem was proposed in principle first in the commonly assigned, copending German patent application Nr. 199 13 067.1 (not prior art), and the loading of further data (printing blocks relating to localities, promotional advertising, carriers) at the vendor by chip card was proposed in principle in the commonly assigned, copending German patent application Nr. 199 13 066.3 (not a prior art). The aforementioned applications have the following titles: Method for the automatic installation of franking devices and arrangement for carrying out the method and Method and arrangement for printing-stamp input into a franking machine, and as far as necessary for a better understanding of this invention, all of the above-mentioned copending disclosures are herewith incorporated by reference.

As outlined in the last paragraph on page 33 of the specification, line 24, the invention is not restricted to the present embodiment. Rather, a number of variants are conceivable within the scope of the claims. For instance,

further other configurations of the invention, based on the same basic idea of the invention and covered by the attached claims, can obviously be developed or used.

Grounds of Rejection to be Reviewed on Appeal

1. Whether or not claims 1-27 are obvious over Leon (US 6,424,954) in view of Vu et al. (US 6,557,104) (hereinafter "Vu") under 35 U.S.C. §103(a).

Argument:

Claims 1 and 18 are independent. Claims 2-17 and 19-27 depend directly or indirectly on claims 1 and 18, respectively. The patentability of claims 4, 24, and 26 are separately argued. Therefore, claims 2, 3, 5, 6, 7-17, 19-23, 25, and 27 stand or fall with claim 1 or 18, but claims 4, 24, and 26 do not stand or fall with claim 1 or 18.

I. Whether or not claims 1-27 are obvious over Leon (US 6,424,954) in view of Vu et al. (US 6,557,104) (hereinafter "Vu") under 35 U.S.C. §103(a).

A. Appellants' claims 1 and 18 are patentable over the cited references.

Before discussing the prior art in detail, it is believed that a brief review of the invention as claimed, would be helpful.

Claim 1 calls for, *inter alia*, a mailing machine assembly, having:

a mailing machine including a controller, a security module connected to the controller, and a non-removable program memory operationally connected to the security module and configured to store an initialization program; and

a removable authorization device operationally connected to the mailing machine and configured to be interrogated by the mailing machine; and

the security module programmed to check whether authorization is present and for preventing an initialization of the mailing machine without authorization. [emphasis added by Applicant]

Appellant's claim 18 includes similar limitations.

The mailing machine according to the present invention is based on a closed system, having a base and a meter, a security module or PSD (Postal Security Device), with the base having a dedicated printer. The present invention provides a mailing machine which overcomes the deficiencies and disadvantages of the prior art devices and methods and has a ROM module with an initialization program, initialization data being introduced in a secure manner into the mailing machine via an externally accessible interface, so that unauthorized initializing is prevented. There is provided a **secure method** without the need to change the ROM module that permits **authorized initialization**.

Thus, according to the present the invention, there is provided a mailing machine assembly, having a mailing machine including a controller, a **security module** connected to the controller, and a non-removable program memory operationally connected to the security module and configured to store an initialization program, and a removable authorization device operationally connected to the mailing machine and configured to be interrogated by the mailing machine, such that the **security module** is programmed to check whether authorization is present and for preventing an initialization of the mailing machine without proper authorization.

The references do not show: (1) "a removable authorization device operationally connected to the mailing machine and configured to be interrogated by the mailing machine ; and (2) the security module programmed to check whether authorization is present and for preventing an initialization of the mailing machine without authorization as recited in independent claim 1 of the instant application. As noted above, independent method claim 18 contains similar features.

More particularly, initialization, in the context of claims 1 and 18, is explained in the specification of the instant

application. For example, paragraph [0012] describes initialization as follows:

"Initialization is understood as meaning a routine for the input of initialization data taking place on one occasion at the single point of entry of the destination country before the machine is put into operation. For this purpose, a means of authorization is brought into operative connection with the mailing machine and is designed as an easily exchangeable electronic hardware unit (dongle or chip card). The latter is connected to the mailing machine either directly or indirectly via a data source, for example a personal computer PC. The mailing machine, for example a franking machine, has an unremovable program memory with an initialization program and a postal security module (postal security device or secure accounting device), which is designed as a means of checking the authorization of the input of initialization data. The latter takes place, when there is authorization, directly by using the keyboard of the franking machine or indirectly via the PC or laptop or from a data center into the meter or security module. The means of authorization, i.e., the authorization device, is brought into operative connection with the meter via interfaces of the PC or the machine. "

For example, paragraph [0007] of the instant application states:

"The object of the present invention is to provide a mailing machine which overcomes the above-noted deficiencies and disadvantages of the prior art devices and methods of this general kind, and which is provided with a ROM module with an initialization program, initialization data being introduced in a secure manner into the mailing machine via an externally accessible interface, so that unauthorized initializing is prevented. It is further intended that a secure method will manage without exchanging the ROM module and permit authorized initialization." [emphasis added by Appellant]

See also, paragraphs [0080] - [0085] of the instant application.

Contrary to Appellant's claimed invention, LEON, does not provide motivation to provide, among other limitations of Appellant's claims, a removable authorization device, authorization from which is necessary for initialization of the mailing machine, as required by Appellant's claims 1 and 18. Rather, In contrast to the closed system of the present invention, Leon discloses an open postage metering system (e.g., see Fig.1B) that includes a host PC 120, a secure meter device(SMD) 150, and a non-dedicated printer 170. A tamper evident enclosure houses the processor and security sensitive elements of the SMD. The printer is coupled to the SMD and is configured to receive and print indicia from the processor. Leon does not disclose a removable authorization device. Nor does Leon show simultaneous operation of two different security systems as recited in the instant claims.

What LEON does disclose is a postage metering system that includes a host PC, an SMD, and a printer. Figs. 1A and 1B of LEON are reproduced herebelow for convenience.

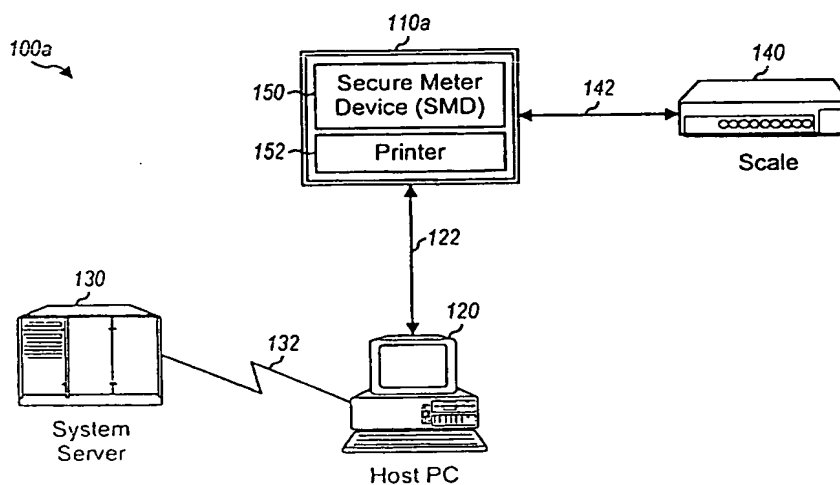


FIG. 1A

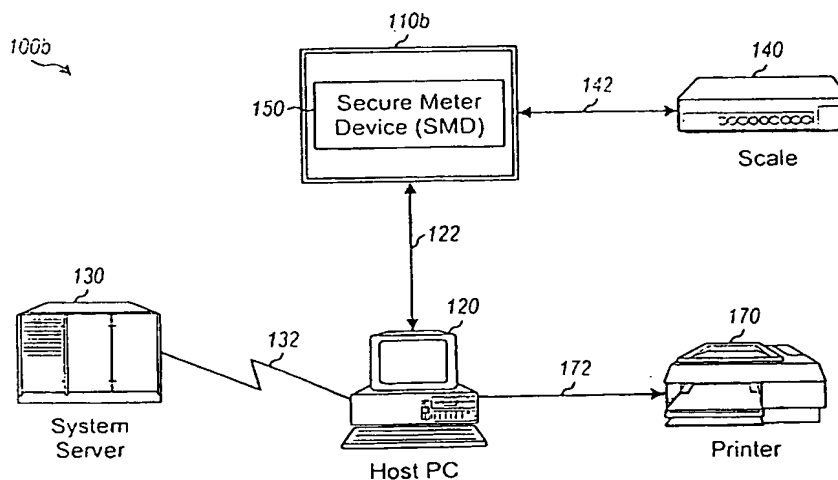


FIG. 1B

As stated on page 3 of the Examiner's Answer, **LEON** fails to disclose Appellant's claimed **removable authorization device**. In fact, **LEON** discloses **initialization** in col. 13, lines 22 - 60, as follows:

Initialization transaction: An Initialization transaction prepares the SMD for operation. The following is a specific implementation of the Initialization transaction, and other implementations are available.

FIG. 5B shows a flow diagram of an embodiment of the Initialization transaction. At a step 520, the SMD is prepared for the Initialization transaction. This preparation can comprise installing a FIT flag located on the SMD. The Crypto-Officer then, via a host PC, sends the SMD an initialization request message that includes the Provider X.509 certificate and the device ID number, at a step 522. This request message is signed using the provider's private key. The SMD receives and validates the request message, at a step 524.

The SMD accepts a request to perform an Initialization transaction if it is in an Uninitialized or Initialized state. This determination is performed at a step 526. If the SMD receives a request to perform an Initialization transaction and the FIT flag is not installed or if the SMD is not in the Uninitialized or Initialized state, the SMD ignores the request and the transaction terminates. The validation of the request message includes verification of the signature in the request message using the provider's public key from the Provider X.509 certificate, at a step 528. If the signature is invalid, the SMD sends an error message, at a step 530, and the transaction terminates.

If the signature is valid, the SMD saves the Provider X.509 certificate provided in the request message, at a step 532. The DSA (digital signature algorithm) parameters p , q , and r are then loaded into the SMD, at a step 534. The SMD uses these parameters to generate a pair of public and provide keys, at a step 536. The SMD retains the private key in secrecy and exports the public key. The SMD sends the host PC a signed message that includes the SMD's public key, at a step 538. This message is signed using the SMD's private key and can be verified by the host PC using the SMD's public key that is included in the message. The SMD then transitions to the Initialized state, at a step 540. Before an initialized SMD leaves the factory, the Crypto-Officer removes the FIT flag and seals the tamper-evident enclosure, at a step 542.

LEON teaches that before an initialized SMD (one containing the key) leaves the factory, the Crypto-Officer removes the FIT flag and seals the tamper-evident enclosure, at a step 542. This is shown in Fig. 5B of LEON, reproduced herebelow, for convenience.

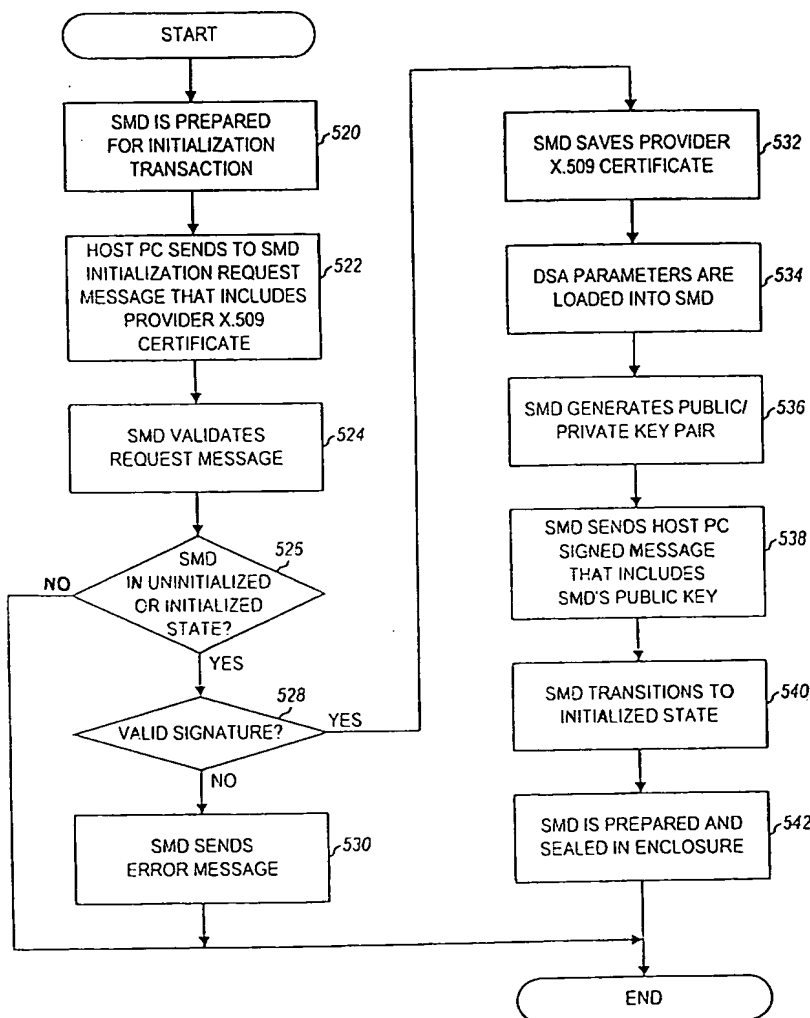


FIG. 5B

Note step 542 of Fig. 5B of LEON; once the enclosure is sealed, initialization ends. See also, Col. 10 of LEON, lines 1 - 9. As can be seen from the foregoing, LEON fails to teach or suggest, or provide any motivation at all, for a removable authorization device, the point of which is to prevent an initialization of the mailing machine without authorization, as claimed by Appellant.

Appellant maintains that, absent impermissible hindsight reconstruction, there is no motivation in either U. S. Patent No. 6,424,954 to Leon "(LEON)" or U. S. Patent No. 6,557,104 to Vu et al ("VU") to combine those references to arrive at Appellant's claimed invention. There is no teaching or suggestion in LEON to use an authorization device for permitting initialization. VU doesn't teach or suggest use in a postal machine.

Rather, VU discloses a method and apparatus for secure processing of cryptographic keys, in which a cryptographic key stored on a token is processed in a secure processor mode using a secure memory. VU does not disclose a security module for checking and preventing an initialization of a mailing machine without authorization. VU's disclosure relates to the field of computer security (International Class H04L 9/32), whereas the present invention and that of LEON relate to the

field of postal meters (International Classes G07B 17/00 and G07B 17/60). The present invention and the prior art disclosures of **LEON** and **VU** are distinctly different on their face as evidenced by their respective distinctly different international classifications and the recitation of the fields to which they relate.. The disclosures of Leon and **VU** are deemed non-analogous and therefore, not properly combinable. There is no motivation or valid basis for combining Leon and Vu other than hindsight reconstruction of the prior art based on appellant's claimed invention. As such, there is no motivation in **LEON** or **VU** to add a method or apparatus for secure processing of cryptographic keys, as taught in **VU**, to the postal system of **LEON**.

However, on page 3 of the Examiner's Answer, it is stated:

"Leon discloses the system components as per the prior Office Action except for the removable authorization device. However, Leon does disclose as per Col. 37, lines 48 - 50, that the Secure Meter Device (SMD) can further include an input interface circuit that couples to an input element. The input element can be a switch, a push button, a key, or the like. The Examiner submits that teaching of the use of an external input element provides the motivation/bridge to incorporate the use of a dongle and/or cryptographic key stored on a token as taught by the second reference Vu in the prior 103 Office Action."

Appellant respectfully disagrees with the above statement from the Examiner's Answer. More particularly, Col. 37 of **LEON**, lines 48 - 50 does not provide motivation to provide, among

other limitations of Appellant's claims, a removable authorization device, authorization from which is necessary for initialization of the mailing machine, as required by Appellant's claims 1 and 18.

As stated in Appellant's Reply Brief, The section of LEON cited in the Examiner's Answer as motivating a combination of LEON with VU to, allegedly, teach Appellant's claimed invention has absolutely nothing to do with initializing the mailing machine, as does the removable authorization device of Appellant's claims. Rather, Col. 37 of LEON, lines 48 - 50, read in the entire context of lines 47 - 60, reads as follows:

"Referring back to FIG. 2A, SMD 150 can further include an input interface circuit 236 that couples via signal line 237 to an input element 238. Input element 238 can be a switch, a push button, a key, or the like. When input element 238 is activated (i.e., by pushing on a print control key), SMD 150 of metering device 110a performs the Indicium transaction. SMD 150 generates an indicium having a predetermined value and directs printer 152 to dispense the indicium. SMD 150 updates its revenue registers when the indicium is generated. SMD 150 generates the indicium when requested and as long as the funds in the revenue registers are sufficient to cover the indicium value. Otherwise, the metering device can indicate a failed Indicium transaction via, for example, a blinking light emitting diode (LED)." [emphasis added by Appellant]

As such, the input element 238 of LEON, cited by the Examiner as the motivation to combine LEON with an external "authorization device" as claimed by Applicants, does not

relate to providing an authorization, based upon which the mailing machine is initialized, as required by Applicants' claims, but, rather, is merely a push button or key used for printing the indicium (i.e., the postage slip). Remember, LEON is sealed at the factory to prevent further access to the key portion. As such, the input element 238 of LEON has nothing to do with authorizing initialization (i.e., as defined in the instant specification) of the postal machine of LEON, as is required of the removable authorization device of Appellant's claims, but merely is used to print the frank, and thus, cannot be said to provide the motivation alleged by the Examiner.

Rather, the LEON reference describes a "funding transaction" which is performed when the indicium register is zero (i.e., no more funds are available for printing an indicium). In LEON, a funding transaction takes place only after initialization is complete. See col. 10 of LEON ("A Registered SMD may be funded by performing a Funding transaction with the system server via the host PC"). For example, , col. 37, lines 32 - 39 of LEON discloses a "funding transaction" described as follows:

"In the stand-alone mode, the metering device is capable of printing as many indicia (i.e., of a predetermined value) as allowed by the funds stored in the SMD. Once the SMD has expended the funds stored

in its revenue registers, it can be loaded with additional funds by performing another Funding transaction. The metering device can then be re-coupled to the host PC for this Funding transaction, and disconnected again after the Funding transaction."
[emphasis added by Appellant]

Although described in connection with the embodiment that uses the input element 238, cited by the Examiner, the input element 238 of LEON is not used in the funding transaction. Rather, the teaching in col. 37, lines 48 - 50 of LEON, read in its entire context, merely provides a motivation for providing a push button or key to print franks (i.e. indicium), which must only necessarily occur after a funding transaction (arguendo, "initialization") has been completed.

As such, Appellant respectfully traverses the allegation in the Examiner's Answer that there is motivation in LEON for Appellant's particularly claimed authorization device.

Further, on page 4 of the Examiner's Answer, it is alleged that:

"The Appellant further argues that Leon is initializing a security module, not the mailing machine as recited in the instant claims. The Examiner submits that the mailing machine has a security module/section that must be initialized before it can function. The kind or type of equipment/machine that is initialized does not render an invention original, unique or non-obvious. The method incorporated to initialize a piece of equipment/machine is what is being presented and

addressed in the prior Office Action." [emphasis added by Appellant]

However, as stated above, Appellant maintains that the LEON reference does not teach or suggest an authorization device, upon which initialization is based. The printing of an "indicium" (i.e., frank or mailing slip) of LEON does not entail "initialization", as claimed by Appellant.

Further, on page 5 of the Examiner's Answer, it is stated that:

"In reference to the Appellant's statement that, ' . . . there is no 'clear and particular teaching or suggestion in Leon to incorporate the features of Vu . . .' the Examiner submits that Leon's [sic] discloses the use of an input element that includes a switch, a key or the like. Col. 37, liners 34-48 [sic]. Vu teaches about a type of key that could be used."

As discussed above, Appellant respectfully disagrees that LEON provides the alleged motivation. The input element of LEON is unrelated to initialization of the mailing machine, as required by Appellant's claims 1 and 18, but is merely used to print out the "indicium". As such, Appellant believes that LEON truly fails to provide the alleged motivation for combining LEON with VU, to disclose Appellant's invention of claims 1 and 18.

Moreover, an open metering system (PC franking system) that would result from a combination of LEON and VU would not meet the claim limitations.

The embodiment of Fig. 1A in LEON shows a postage metering system using an open metering system. Figs. 1A and 2A show a meter 110a having an integrated printer 152. The meter of the present invention is not similar to the meter 110a of the embodiments in Figs. 1A and 2A of Leon. A combination of the features of Vu and Leon results in a meter with an integrated printer in contrast to the present invention having a dedicated printer.

The present invention provides an initialization of a mailing machine, and not of the security module or PSD (Postal Security Device) as disclosed in LEON. LEON discloses in cols. 12-13 and 26, Figs. 5a, 5b and 6b in particular, an initialization of the security module, not the mailing machine as recited in the instant claims.

B. Appellants' claim 4 is patentable over the cited references.

Also, in contrast to claim 4, Leon does not disclose "a postal security device configured to check an authorization of the

data input" as recited in the claim 4 of the instant application.

C. Appellants' claims 24 and 26 are patentable over the cited references.

Claims 24 and 26 positively recite the features "a data input sending the notification by the telepostage data center TDC including extra data stored in a non-volatile memory externally of the security module and including inkjet cartridge data" and "providing data input of extra data including inkjet cartridge data and storing the data in a non-volatile memory externally of the security module", respectively. Neither of these limitations is shown in LEON as acknowledged by the Examiner.

II. Conclusion

It is well-settled that almost all claimed inventions are but novel combinations of old features. The courts have held in this context, however, that when "it is necessary to select elements of various teachings in order to form the claimed invention, we ascertain whether there is any suggestion or motivation in the prior art to make the selection made by the applicant". Interconnect Planning Corp. v. Feil, 227 USPQ 543, 551 (Fed. Cir. 1985) (emphasis added). "Obviousness can

not be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching, suggestion or incentive supporting the combination". In re Bond, 15 USPQ2d 1566, 1568 (Fed. Cir. 1990). "Under Section 103 teachings of references can be combined **only** if there is some suggestion or incentive to do so." ACS Hospital Systems, Inc. v. Montefiore Hospital et al., 221 USPQ 929, 933, 732 F.2d 1572 (Fed. Cir. 1984) (emphasis original). "Although a reference need not expressly teach that the disclosure contained therein should be combined with another, the showing of combinability, in whatever form, must nevertheless be '**clear and particular.**'" Winner Int'l Royalty Corp. v. Wang, 53 USPQ2d 1580, 1587, 202 F.3d 1340 (Fed. Cir. 2000) (emphasis added; citations omitted); Brown & Williamson Tobacco Corp. v. Philip Morris, Inc., 56 USPQ2d 1456, 1459 (Fed. Cir. Oct. 17, 2000). Appellants believe that there is no "clear and particular" teaching or suggestion in Leon to incorporate the features of Vu as suggested by the Examiner.

In establishing a *prima facie* case of obviousness, it is incumbent upon the Examiner to provide a reason why one of ordinary skill in the art would have been led to modify a prior art reference or to combine reference teachings to arrive at the claimed invention. Ex parte Clapp, 227 USPQ 972, 973 (Bd. Pat. App. & Int. 1985). To this end, the

requisite motivation must stem from some teaching, suggestion, or inference in the prior art as a whole or from the knowledge generally available to one of ordinary skill in the art and not from the *applicant's* disclosure. See, for example, Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 1052, 5 USPQ2d 1434, 1439 (Fed. Cir. 1988), *cert. den.*, 488 U.S. 825 (1988). It is respectfully submitted that the Examiner has not provided the requisite reason why one of ordinary skill in the art would have been led to modify Leon or to combine Leon's and Vu's teachings to arrive at the claimed invention for providing a mailing machine assembly as recited in the instant claims. Further, the Examiner has not shown the requisite motivation from some teaching, suggestion, or inference in Leon or Vu or from knowledge available to those skilled in the art.

Appellant respectfully believes that any teaching, suggestion, or incentive possibly derived from the prior art is only present with hindsight judgment in view of the claimed invention. "It is impermissible, however, simply to engage in a hindsight reconstruction of the claimed invention, using the applicant's structure as a template and selecting elements from references to fill the gaps. The references **themselves** must provide some teaching whereby the applicant's combination would have been obvious." In re Gorman, 18 USPQ2d 1885, 1888

(Fed. Cir. 1991) (emphasis added). In the instant rejection, no such teaching is present in or apparent from the cited prior art references.

Upon evaluation of the Examiner's response and statements, it is respectfully believed that the evidence adduced by the Examiner is insufficient to establish a prima facie case of obviousness with respect to the claims. Accordingly, the Honorable Board is therefore requested to reverse the final rejection of the Supervisory Primary Examiner.

The Honorable Board is therefore respectfully urged to reverse the final rejection of the Examiner.

Respectfully submitted,

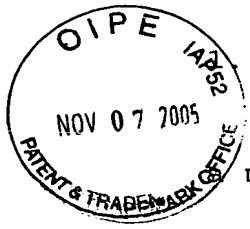


Kerry P. Sisselman (37,237)

FDP/bb

Date: November 4, 2005
Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, Florida 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

Claims Appendix:



A mailing machine assembly, comprising:

mailing machine including a controller, a security module connected to said controller, and a non-removable program memory operationally connected to said security module and configured to store an initialization program; and

a removable authorization device being operationally connected to said mailing machine and configured for being interrogated by said mailing machine; and

said security module being programmed to check whether authorization is present and for preventing an initialization of said mailing machine without authorization.

2. The mailing machine assembly according to claim 1, wherein said authorization device is indirectly connected to said mailing machine via a data source selected from a group consisting of a personal computer, a laptop, and a remote data center.

3. The mailing machine assembly according to claim 1, wherein said authorization device is directly connected to said mailing machine.

4. The mailing machine assembly according to claim 2, wherein said mailing machine is a franking machine having a meter with a user interface, for a data input of predetermined values, and a postal security device configured to check an authorization of the data input.

5. The mailing machine assembly according to claim 4, wherein said franking machine has a base with a first interface for attachment of said data source containing initialization data for said mailing machine, and a second interface for attachment of said authorization device.

6. The mailing machine assembly according to claim 5, wherein said authorization device is a dongle.

7. The mailing machine assembly according to claim 5, wherein said data source contains initialization data for said mailing machine and is configured to be attached to said first interface of said base of said mailing machine, and wherein said authorization device is a chip card and a chip card reader is operatively connected to said meter via a further internal interface and arranged to be integrated into said base.

8. The mailing machine assembly according to claim 5, wherein said first, second and further interfaces of said mailing machine are serial interfaces.

9. The mailing machine assembly according to claim 4, wherein said interface is a serial interface.

10. The mailing machine assembly according to claim 5, wherein said first interface of said base of said mailing machine is configured for attachment of said data source, said authorization device is connected to said data source via a parallel interface, said data source is a computer and is coupled via a serial interface of said mailing machine, and wherein a chip card reader is integrated and operatively connected to said meter via an interface of said meter.

11. The mailing machine assembly according to claim 1, wherein said mailing machine is a franking machine with a meter and a chip card reader integrated in said meter and coupled to a parallel bus of said meter via an interface and wherein said authorization device is a chip card.

12. The mailing machine assembly according to claim 1, wherein said mailing machine is a set of scales, and wherein

a chip card reader is integrated into said scales and coupled via an interface of said scales, and wherein said authorization device is a chip card.

13. The mailing machine assembly according to claim 1, wherein said mailing machine has a modem and a modem interface for loading therethrough the initialization data or values, and wherein said authorization device is an insertable chip card, for authorizing at least that part of the initialization data which are loaded into said mailing machine from a data source via said modem interface.

14. The mailing machine assembly according to claim 1, wherein said mailing machine is a franking machine having at least one program memory with an initialization program and a postal security module, for checking the authorization before and during the initialization, and wherein said postal security module is configured for loading initialization data.

15. The mailing machine assembly according to claim 14, wherein a checking of the authorization before and during the initialization is performed on the basis of a unique authorization number, input via a dongle or a chip card and

wherein the authorization is given if the unique authorization number input into the mailing machine has a predetermined relationship with a number stored in said postal security module.

16. The mailing machine assembly according to claim 1, which comprises a program memory at least partly storing the initialization program, said program memory forming a component part of said security module, and including a separate program memory operatively in connection with said security module and storing another part of the initialization program.

17. The mailing machine assembly according to claim 16, wherein the other part of the initialization program is for initialization data stored in a non-volatile manner externally of the security module.

18. A method of initializing a mailing machine, which comprises the steps of:

switching a mailing machine into an initialization mode;

authorizing an initialization with an authorization device and checking authorization with a security module, in order to prevent initialization without authorization;

if authorization is found, inputting initialization data at least partly supplied by a data source; and

ending the initialization and cancelling of the authorization.

19. The method according to claim 18, which comprises:

switching a franking machine into the initialization mode and establishing a connection to a data source;

authorizing initialization with an authorization device;

inputting a battery date BAT_DATE_SAD of a battery of the security module, a telephone number of the telepostage data center TDC of the destination country and a postage call-up number PAN;

transmitting a serial number SAD-SN of the security module to the telepostage data center TDC of the country, to initialize a comparison of the serial number SAD-SN sent with a stored serial number, and to generate a notification;

receiving the notification sent by the telepostage data center TDC in the franking machine and loading codes DES-Keys for credit recharging into the security module SAD; and

terminating the initialization and cancelling the authorization by removing the authorization device.

20. The method according to claim 19, wherein the establishing step comprises connecting via a transmission device selected from a group consisting of a modem, a laptop, and a PC interface.

21. The method according to claim 19, which comprises switching into the initialization mode at the goods

receiving location in the destination country as a result of activating a means of activating a user interface and establishing a connection to a data source via a transmission device selected from the group consisting of a modem, a laptop, and a PC interface.

22. The method according to claim 19, comprising sending notification by the telepostage data center TDC including a code MAC-Key for a security imprint, which is received by the franking machine and loaded into the security module SAD.

23. The method according to claim 19, comprising providing the codes DES-Keys for credit recharging including the subcodes Key(0), Key(1), Kvar and loading the codes into the security module SAD.

24. The method according to claim 23, comprising sending the notification by the telepostage data center TDC including extra data stored in a non-volatile memory externally of the security module and including the inkjet cartridge data.

25. The method according to claim 18, wherein the inputting step comprises inputting initialization data with the chip card.

26. The method according to claim 18, comprising providing data input of extra data including inkjet cartridge data and storing the data in a non-volatile memory externally of the security module.

27. The method according to claim 18, which comprises interrogating the authorization device before and during the initialization of the mailing machine with predetermined data.

Evidence Appendix

No Evidence under 37 C.F.R. §§ 1.130, 1.131 or 1.132 were submitted and relied upon by Appellants in the present appeal.

Related Proceedings Appendix:

There are no related proceedings identified in the related appeals and interferences section or decisions rendered by a court or the Board.